

REPORT DOCUMENTATION PAGE

AFRL-SR-BL-TR-00-

Public reporting burden for this collection of information is estimated to average 1 hour per response, including gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Service, Paperwork Project, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Project, Suite 1204, Arlington, VA 22202-4302.

data sources
aspect of this
215 Jefferson

0395

1. AGENCY USE ONLY (Leave Blank)		2. REPORT DATE March 1, 2000		3. REPORT TYPE AND DATES COVERED Final Technical Report 1 March 1999 - 29 February 2000	
4. TITLE AND SUBTITLE Computer Network Equipment for Intrusion Detection Research				5. FUNDING NUMBERS G F49620-99-1-0135	
6. AUTHORS Nong Ye					
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Arizona State University Box 871603 Tempe, AZ 85287-1603				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) AFOSR/NM 801 N. Randolph St Arlington, VA 22203-1977				10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES					
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release				12b. DISTRIBUTION CODE	
13. ABSTRACT (Maximum 200 words) A set of computer and network equipment has been purchased to support the intrusion detection research. The objective of the intrusion detection research currently funded by AFOSR is to investigate, develop and test: 1) A process model of computer and network operation to capture computer and network activities to a full range from individual components of a computer and network system to the system itself at multiple levels of abstraction; 2) Model-based intrusion detection techniques at the system level to detect coordinated actions and interactive effects of intrusion by correlating and intrusion likelihood values from component-level intrusion detection techniques; and 3) A working prototype of an intrusion detection system to detect intrusions through the integration of the process model and intrusion detection techniques. To test the process model, the system-level intrusion detection techniques and the working prototype of the intrusion detection system, a set of computer and network equipment has been purchased through this grant to construct a computer and network system that represents a typical DoD information infrastructure involving a mix of different machines and operating environments. Specifically, the following have been purchased: <ul style="list-style-type: none"> three Sun workstations one Silicon Graphics workstation one Dec workstation four Micron PCs two Macintosh PCs. 					
14. SUBJECT TERMS Intrusion detection information security				15. NUMBER OF PAGES 2	
				16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL		

Final Report to AFOSR

GRANT NO.: F49620-98-1-0257
PROJECT TITLE: DURIP: Computer Network Equipment for Intrusion Detection Research
PI: Nong Ye
REPORTING PERIOD: March 1, 1999 – February 29, 2000

A set of computer and network equipment has been purchased to support the intrusion detection research. The objective of the intrusion detection research currently funded by AFOSR (grant #: F49620-99-1-0014) is to investigate, develop and test:

- 1) A process model of computer and network operation to capture computer and network activities to a full range from individual components of a computer and network system to the system itself at multiple levels of abstraction;
- 2) Model-based intrusion detection techniques at the system level to detect coordinated actions and interactive effects of intrusion by correlating and intrusion likelihood values from component-level intrusion detection techniques; and
- 3) A working prototype of an intrusion detection system to detect intrusions through the integration of the process model and intrusion detection techniques.

To test the process model, the system-level intrusion detection techniques and the working prototype of the intrusion detection system, a set of computer and network equipment has been purchased through this grant. Specifically, the following have been purchased:

- three Sun workstations
- one Silicon Graphics workstation
- one Dec workstation
- four Micron PCs
- two Macintosh PCs.

The above machines and existing equipment in the lab are used to form a computer and network system that represents a typical DoD information infrastructure involving a mix of different machines and operating environments. This computer and network system is shown below. The computer and network system consists of a protected network domain and an outside network domain which are connected through a Cisco router. Figure 1 shows the architecture of the computer network system as well as the description, role and ID of each machine in the system. The protected domain contains the UNIX server and clients, the Windows NT server and clients, the UNIX security server, and the Windows NT security server. The outside domain contains two UNIX-based workstations and three PCs.

This computer and network system has been used to test the process model, intrusion detection techniques and the working prototype of an intrusion detection system that have been and are being developed under the three year AFOSR grant (grant #: F49620-99-1-0014).

